


Predicting and Explaining Cyber Ethics with Ethical Theories

Winfred Yaokumah, University of Ghana, Accra, Ghana

 <https://orcid.org/0000-0001-7756-1832>

ABSTRACT

People face multiple decisions that have ethical dimensions and are often unable to resolve appropriately those ethical dilemmas in the use of the cyberspace. Individuals find it difficult to explain the rationale behind their moral judgments in their interactions and access to digital content. Identifying ethical and moral orientation that prompts acceptable or unacceptable ethical judgments is an important factor in cyber ethics. The goal of this study is to employ three prominent ethical theories to predict and explain cyber ethical judgements in terms of computer ethics, privacy, intellectual property rights, and academic integrity. The study develops conceptual and predictive models to test a set of hypotheses. The results show consequential ethics as the most significant predictor of computer ethics, cyber privacy, and academic integrity. Deontological ethics most significantly predict intellectual property rights but is not a significant predictor of academic integrity.

KEYWORDS

Academic Integrity, Consequentialism, Cyber Ethics, Cyber Security, Deontology, Ethical Theory, Intellectual Property, Piracy, Plagiarism, Privacy, Virtue Ethics

INTRODUCTION

Individuals face ethical dilemmas in various real-life situations and often make ethical judgments based on what they deem to be right or wrong. Ethics is a set of principles by which people live; what they consider as morally right or wrong; their judgments about what ought to be done; and about moral duties and obligations people should perform (Heller, 2012). Digital transformation through the use of information and communication technologies, though improves critical business operations and economic growth, poses ethical challenges to the society (Tiirmaa-Klaar, 2016). In particular, interactions among people and access to digital content in the cyberspace bring ethical concerns (Jamal et al., 2015). Some decisions and choices individuals make in the cyberspace are unethical or illegal (Luppardini, 2009). Often, individuals are unable to resolve ethical dilemmas (Arar et al., 2016). In some cases, people find it difficult to explain the rationale behind their moral judgments in their accessibility and interactions with digital content. It is often hard to conclude what ought to be the most appropriate ethical behaviour. This is because differences exist among individuals in their judgements and even among cultures as to what is right or wrong (Burmeister, 2017).

Ethics in the cyberspace is often referred to as cyber ethics. Cyber ethics is a term used to encompass all forms of applied ethics issues pertaining to technology related human activities (Luppardini, 2009). Cyber ethics tries to determine an appropriate perspective or philosophy in the application of technology to real-life situations (Shapiro & Gross, 2013). Ethical theories are useful when faced with alternative perspectives for evaluating and resolving ethical situations (McDonald,

DOI: 10.4018/IJCWT.2020040103

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

2014). As people face multiple decisions that have ethical dimensions in the cyberspace, it is important to establish what ethical theoretical perspectives and moral convictions that prompt acceptable or unacceptable ethical judgments. Ethical theories enable individuals to defend or oppose a position on a particular ethical issue (Hammersley-Fletcher, 2015) in the cyberspace. According to Amin (2019), providing cyber safety requires four interrelated domains: a) hardware, software, and networks as building blocks of the organization's cyber infrastructure; b) the information domain which includes monitoring, information storage, and visualization; c) the cognitive domain which involves information analysis for decision-making; and d) the social domain where appropriate social and ethical considerations are made.

This current study focuses on the ethical domain of cyber security to predict and explain cyber ethics using ethical theories. Literature suggest that among several ethical theories, consequentialism, deontology (Heller, 2012) and virtue ethics (Audi, 2015) are the most relevant to technological applications. Consequentialism (consequence-based ethics) refers to those moral theories which hold that the consequences (i.e. outcomes) of a particular action form the basis for any valid moral judgment about that action or create a structure for judgment (Sinnott-Armstrong, 2014). Deontological ethics (duty-based ethics) are concerned with what people should do, not with the consequences of their actions (Alexander & Moore, 2015). It focuses on doing the right thing because it is the right thing to do (Alexander & Moore, 2015). Virtue ethical theory (character-based ethics) focuses on the criteria having to do with character development of individuals and the acquisition of good character traits (Hinmann, 2016). This study employs these three prominent ethical theories to predict and explain ethical judgements of individuals in the use of the cyberspace. The question the study attempts to answer is "How do ethical theories predict and explain cyber ethics?" Empirical evidence to predict and explain the effect of ethical theories on cyber ethics is lacking in the literature. As a consequence, full ethics is needed in the field of cyberspace (Dipert, 2016) and more research is required to explore appropriate ethical theories that can foster cyber ethics (Burmeister, 2017).

LITERATURE REVIEW

Ethical Theories

Ethical theories are generally categorized into three: Consequentialism, deontology, and virtue ethics (ethics of character). Consequentialism and deontology answer a question as to "how should I act?" and the virtue ethics answer a question as to "what kind of person ought I to be?" (Hinmann, 2016).

Consequentialism

Consequential ethics contends that people should strive to maximize positive outcomes (Sinnott-Armstrong, 2014). It is based on two principles: (a) whether an act is right or wrong depends only on the results of that act and (b) the more good consequences an act produces, the better or righter that act (Ethics guide, 2014). Consequentialism is categorized into utilitarianism, group consequentialism, and ethical egoism (Hinmann, 2016). For utilitarianism, an action is right if it tends to promote happiness and wrong if it tends to produce reverse of happiness (Driver, 2014; Mill, 1961). With this view, an act is morally permissible if the consequences resulting out of it produces greatest amount of good for the greatest number of persons affected by the act (Sinnott-Armstrong, 2014). Utilitarianism plays a very important part in everyday life because it is simple and appeals to common sense: (a) It seems sensible to base ethics on producing happiness and reducing unhappiness, (b) It seems sensible to base ethics on the consequences of what is done, since people usually take decisions about what to do by considering what results will be produced, and (c) It seems easy to understand and which is based on common sense (Ethics guide, 2014). Another aspect of consequentialism is group consequentialism, which considers consequences of an act on smaller groups such as a nation, a tribe, a family, or

fellow believers. The third aspect of consequentialism is ethical egoism, which focuses only on the consequences of an action on oneself (Hinmann, 2016).

Consequential ethics play a vital role in decision-making in the cyberspace (Heller, 2012) and can guide, predict, or explain ethical decisions of individuals. In particular, in the current era there are numerous laws and regulations that protect digital content. Examples are the cyber privacy regulations (Data Protection Commission, 2012), intellectual property rights (Copyright Act, 2005), and other laws against cybercrime and terrorism. In the face of the punitive measures from these laws, people may consider the consequences of their actions when making ethical decisions regarding cyber privacy infringement, committing cybercrime, violating academic integrity, or infringing on intellectual property rights. Therefore, consequences of decisions made in the cyberspace may predict and explain cyber ethics of individuals.

Deontology

Deontology is a rule-based ethic focused not on the consequences of the actions but on the inherent wrongness of the acts themselves (Alexander & Moore, 2015; Kant, 1993). Deontological ethics focus on moral obligations and adherence to moral principles and prescribed rules (Hinmann, 2016). Moral duties prescribe things which are right to do or which are wrong to do. The theory argues that whether something is right or wrong depends on the act itself. Kant's theory is an example of a deontological moral theory. According to this theory, the rightness or wrongness of actions does not depend on their consequences but on whether they fulfil our duty (Kant, 1993). Kant believes that there is a supreme principle of morality and refers to it as the categorical imperative (Kant, 1993). Deontology proposes that to act ethically, one ought to follow the appropriate rules (universal moral laws) that one ought to do to perform one's duty (Kant, 1998). Therefore, the right course of action is the performance of one's duty, which determines what is good or wrong.

In view of this individual's ethical decision may be based on the allegiance to a code of conduct. Institutions and organizations have ethical codes of ethics (Computer Ethics Institute, 1992; Association for Computing Machinery, 2018) to guide the conducts of members in the use of the cyberspace. In particular, there is a code of ethics in academia with respect to plagiarism, in which students, instructors and researchers should abide by. These codes of ethics act as the appropriate rules that individuals ought to follow to perform their duties. Even the society as a whole is guided by a code of ethics for everyone to perform moral duties (Computer Ethics Institute, 1992). In this regard people owe it a duty to act ethically. This may inform their decisions regarding committing cybercrime, infringing on others privacy, or violating intellectual property rights.

Virtue Ethics

Virtue ethics concentrate on the person rather than the action. It looks at the moral character of the person carrying out an action and is more concerned with the development of character (NASUTI, 2018). Virtue ethics propose that the best way to guarantee the right actions is to ensure that individuals have strong character, the virtues appropriate to the situation (Hinmann, 2016). It is often regarded an agent-oriented theory which emphasizes on being a moral person through proper training for acquiring moral virtues (Monteverde, 2014). It places emphasis on being rather than doing. One reason why virtue ethics can be popular and why they make an important contribution to our understanding of morality is that they emphasize the central role played by motives in moral questions (Hinmann, 2016). The earlier works of Aristotle underpinned ethics of character. Aristotle viewed virtues as strengths of character necessary for human flourishing and vices as weaknesses of character that would impede such flourishing (Ethics guide, 2014). Audi (2015) believes that a person of good character (virtue ethics) will be able to discern the morally best course of action (Audi, 2015). Therefore, a person of moral character will do the right thing by not violating others privacy, unlawfully appropriating others intellectual property, or infringing on others privacy in the cyberspace.

Cyber Ethics

Technological advances in social media platforms, virtual reality, and augmented reality technologies bring about ethical consequences (Churchill, 2019). Digital devices enable creation, storage and duplication of data, providing an avenue for distributing digital content (Luppardini, 2009). As the use of the cyberspace comes with numerous benefits, it has a profound negative impact on society, businesses and governments (Onyancha, 2015) in the area of cyber ethics. Cyber ethics encompass a wide range of activities, including computer ethics (such as cybercrime, cyber fraud, spreading of ransomware, cyber terrorism, and cyberattacks), cyber privacy, intellectual property rights (digital piracy protection), and academic integrity (protection against plagiarism and academic dishonesty).

Computer Ethics

Computer ethics relate to practical and everyday problems arising from the use of computers and computer networks (Stamatellos, 2011). As the types of network connectivity and volumes of data flow increase, the potential for cyber-attacks (Dupont, 2013) and misuse of computer resources increase. Cyber-attacks include unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and physical infrastructure used to process, communicate and store information (Abu-Shaqra & Luppardini, 2016). A recent report shows an increase in computer related crimes against individuals, businesses, and infrastructure. Cybercrimes cause a sizable loss to the world economy (Hayman, 2013). For example, Cybersecurity Ventures (2019) predicts that cybercrime damages will cost the world about \$6 trillion by 2021. Attacks on computer systems comprise of advanced persistent threats, social engineering, insider threats, and attacks on network infrastructure (Happa & Goldsmith, 2017). Critical infrastructure, such as power generation and distribution systems, telecommunications networks, military installations, transportation control networks, financial networks, and government information and communications technology (ICT) are increasingly becoming the target for cyberattacks (Miron & Muita, 2014). Cyber attackers or hackers can disrupt banking and financial services, energy supply, air traffic control, and major industries (Lonsdale, 2016). Hackers seek and exploit weaknesses in computer systems or networks (Engbretonson, 2011). They can compromise the confidentiality, integrity, or availability (CIA) of information systems. This brings greater focus on the security of information resources and the protection of critical infrastructures in the cyberspace.

Cyber Privacy

Privacy is the right to be anonymous (Dunne, 2009) and the right to be left alone (Shiffrin, 2016). The right to be anonymous is a form of privacy that has particular significant implication in the cyberspace (Dunne, 2009). Privacy is a condition under which a person can live without intrusion and scrutiny of others (Shiffrin, 2016). It enables the development of one's own independent personality, the sense of creativity, and critical sensibilities and substance (Shiffrin, 2016). Lack of privacy inhibits innovation and independence, making a person to conform or succumb to social construction (Shiffrin, 2016). Keeping secrets and maintaining privacy are key principles of security, but privacy violation is at stake as an increasing number of private data are uploaded to the cloud daily (García-Matos & Torner, 2015). According to Barger (2008), everyone should have something to hide; including personal information which when revealed can be used for identity theft or other kinds of fraud. But should every information about a person be private? Nevertheless, privacy is about when, where, and how information about a person is used and by whom (Buttyán & Hubaux, 2007). Hiding personal information from unauthorized parties is very important, but revealing personal information to authorized parties under well-defined circumstances can be very useful (Buttyán & Hubaux, 2007). Cyber privacy spans personal or organizational data. There are frequent occurrences of security breach and invasion of privacy, ransomware, and widespread breaches of private data (Hennig, 2018). The popularity of technology that facilitates communications through the use of blog, twitter, and other social networking media such as Facebook and MySpace enable individuals to share ideas, jokes, pictures, video, and music. These technologies endanger privacy in the cyberspace.

Intellectual Property

Downloading copyrighted materials without paying is considered the main practice of piracy (Tomczyk, 2019). Cyber piracy gives financial benefits to perpetrators through downloading of and the sale of copyrighted materials such as music, videos, games, and software (Taylor, 2012). The negative implication of downloading copyrighted materials illegally from the Internet is the financial loss it causes to the owners. Therefore, cyber piracy is often labelled as theft and may result in legal liability (Tomczyk, 2019). Patent and copyright laws play an important role in providing legitimate protection for the originators to intellectual property rights and make it possible for them to recoup development costs and exploit legitimate competitive advantage (Schultz, 2010). Despite the growth of legitimate content sites, the volume of pirated movies, TV shows, music, books and video games online continues to grow at a rapid pace (Verrier, 2013). For example, a report suggests that 92% of e-book readers in Russia got their books through illegal downloads, while in the US the e-book piracy rate was about 12% (Indvik, 2013). In spite of the legal protections for digital content, users continue to pirate digital content as they rationalize their behaviour (Moore & McMullan, 2009). Charoensukmongkol et al. (2012) suggest that improvement in economic wealth of people can reduce piracy.

Academic Integrity

Academic integrity is an intellectual honesty composed of professional code serving academia, including students, instructors, and researchers. Academic dishonesty, also sometimes refers to as plagiarism, is the breach of journalistic ethics of “wrongful appropriation” and “stealing and publication” of another author’s “language, thoughts, ideas, or expressions” and the demonstration of them as one’s original work (Dhusia, 2017). Academic integrity embodies honesty, trust, fairness, respect and responsibility in the use of others’ work (Swartz & Cole, 2013). But, academic dishonesty has been a problem in higher education (Sulphrey & Jnaneswar, 2013), particularly as the result of access to content in the cyberspace. It is also a problem in the classroom as well as in an online setting (Perez-Pena, 2012). Sulphrey and Jnaneswar (2013) find significant correlation between academic dishonesty and unethical behaviour. In a recent survey, eighty-two of the college undergraduates reported having cheated (Novotney, 2011). In a survey of college and high school students with respect to academic dishonesty, as high as 75-95% of college students and nearly 75% of high school students admitted to academic dishonesty (Executive Summary of the National Cyberethics, 2009).

Conceptual and Predictive Model

This section compares and contrasts ethical theories and integrates them with cyber ethics in order to propose a conceptual model, based on which the hypotheses are stated. With ethical theories in current use, ethicists squabble about how to rank these theories. Deontological ethics is an approach to ethics that focuses on the rightness or wrongness of action itself as opposed to the rightness or wrongness of the consequence of the action (consequentialism) or to the character and habits of the actor (virtue ethics). For consequentialism, the consequence determines what is right. It suggests that when faced with a moral dilemma a person should choose the action that maximises good consequences (Driver, 2014; Mill, 1961). While it sounds attractive in theory, consequentialism is a very difficult theory to apply in real life moral decisions because it ignores things regarded as ethically relevant. Consequentialism is only interested in the consequences of an act (Hinmann, 2016); the intentions of the person doing the act are irrelevant (Ethics guide, 2014). So, an act with good results done by someone who intended harm is as good as if it was done by someone who intended to do good. Also, the past actions of the person doing the act are irrelevant, the character of the person doing the act is irrelevant, and the fairness of the consequences is not directly relevant (Ethics guide, 2014). In view of these, to what extent do people consider the consequences of an act in the cyberspace?

For Deontological ethics the right cause of action (duty) determines the right (Alexander & Moore, 2015). Many religious practices maintain that duty determines what is good and regards

natural law as supreme without recourse to the consequences. Often, ethics of duty is seen in military contexts, where it is important to do the right thing, regardless of the consequences (Hinmann, 2016). Professional code of ethics is an example of deontological ethics. Organizations and IT professional bodies such as Association for Computing Machinery (ACM) and Computer Ethics Institute (CEI) spell out ethical conducts that define how members should behave when faced with ethical decisions. These ethical codes of conduct are focused mainly on the technology related ethics, including privacy, academic integrity, piracy, and cybercrime. State institutions also define privacy and piracy laws to restrain people from unethical behaviour. But, to what extent do these codes of ethics influence cyber ethics behaviour.

Now, claiming either that consequential ethics is superior to virtue ethics or the reverse would be controversial. Yet without consensus about which theories are better or worse, how can progress be measured? (Ethics guide, 2014). According to Talbot (2012), each theory has merits and demerits and their application should be balanced against each other when deciding how to act. Spinello and Tavani (2004) suggest that a more comprehensive theory combining the strengths of existing ethical theories should be developed. Based on this discussion, the current study proposes the combining of three prominent ethical theories to ascertain the significant role they play in ethical decisions of people in the cyberspace. The conceptual model establishes the relationship between ethical theories and cyber ethics (computer ethics, intellectual property rights, academic integrity, and cyber privacy). Figure 1 suggests that consequence-based ethics, duty-based ethics, and character-based ethics will predict cyber security, cyber privacy, academic integrity, and intellectual property right. The study puts forward four hypotheses and four predictive regression models:

Hypothesis 1: Consequential ethics, Deontological ethics, and Virtue ethics will significantly predict and explain computer ethics.

Model 1: Computer Ethics (CET) = $\beta_0 + \beta_1 \text{CBE} + \beta_2 \text{DBE} + \beta_3 \text{VBE} + \varepsilon$

Hypothesis 2: Consequential ethics, Deontological ethics, and Virtue ethics will significantly predict and explain cyber privacy.

Model 2: Cyber Privacy (PRI) = $\beta_0 + \beta_1 \text{CBE} + \beta_2 \text{DBE} + \beta_3 \text{VBE} + \varepsilon$

Hypothesis 3: Consequential ethics, Deontological ethics, and Virtue ethics will significantly predict and explain intellectual property rights.

Model 3: Intellectual Property (IPR) = $\beta_0 + \beta_1 \text{CBE} + \beta_2 \text{DBE} + \beta_3 \text{VBE} + \varepsilon$

Hypothesis 4: Consequential ethics, Deontological ethics, and Virtue ethics will significantly predict and explain academic integrity.

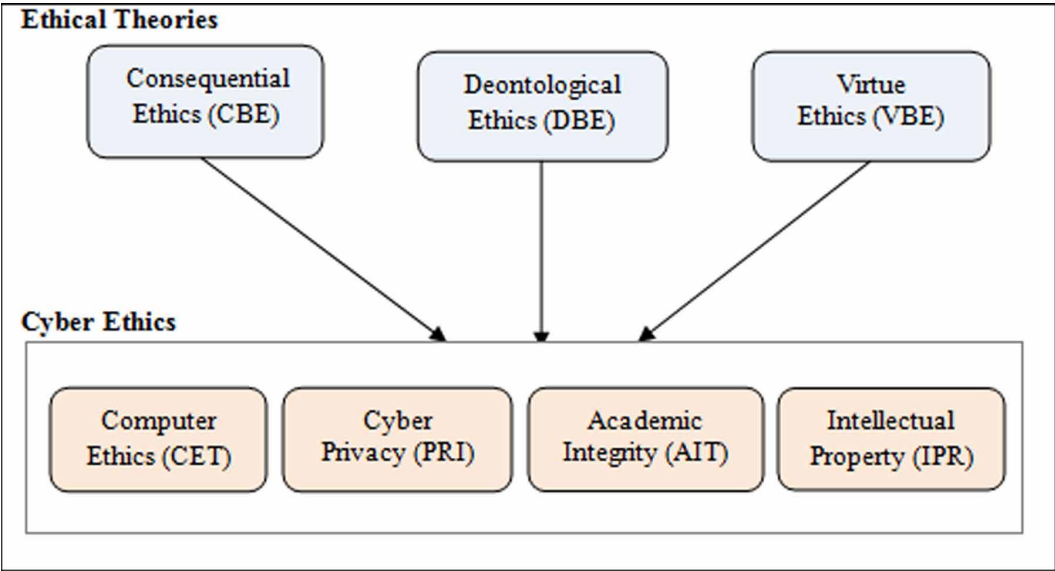
Model 4: Academic Integrity (AIT) = $\beta_0 + \beta_1 \text{CBE} + \beta_2 \text{DBE} + \beta_3 \text{VBE} + \varepsilon$

In the models, β_0 is a constant; β_1 , β_2 and β_3 represent the slope (regression coefficients), and ε is any other factor that may impact cyber ethics but not included in the model, CBE is Consequence-Based Ethics; DBE is Duty-Based Ethics; and VBE is Virtue-Based Ethics.

METHODOLOGY

The study used a quantitative research design. The population of interest was students in universities in Ghana and the sample frame was the universities located in five regional capitals. The participants were selected because they have regular access to the Internet and are faced with cyber ethical decisions in the course of their studies. Stratified sampling was employed to classify the population into private and public universities. Five public and three private universities were selected since they have a charter status. Following, a simple random sampling strategy was used to select the samples from the sample frame. Two cyber ethics instruments were adopted from Computer Ethics Institute (Computer Ethics Institute, 1992) generally referred to as the Ten Commandments of Computer Ethics

Figure 1. A model of ethical theories and cyber ethics



and the Questionnaire for Ethical Perceptions (Omosalewa, Aasheim, & Rutner, 2013). The items on the questionnaire used a 5-point Likert scale (Strongly disagree = 1, Disagree = 2, Not Sure = 3, Agree = 4, and Strongly agree = 5) to assess the respondents' responses concerning the degree of their ethical theoretical orientation on cyber ethics constructs.

The reliability of the instruments was tested using Cronbach's alpha. The Computer Ethics subscale consisted of 5 items (Alpha = .88), the Cyber Privacy subscale consisted of 5 items (Alpha = .85), the Intellectual Property subscale consisted of 3 items (Alpha = .78), and the Academic Integrity subscale consisted of 8 items (Alpha = .88). Moreover, the Cronbach's alphas for the ten Consequential Ethics items, ten Deontological Ethics items, and ten Virtue Ethics items were .88, .90 and .92 respectively (see Table 7 in Appendix A). According to Henseler and Sarstedt (2012), an alpha of .7 is an acceptable indicator of reliability. Therefore, all the constructs on the instrument were found to be highly reliable. The data analysis was conducted using multiple regression analysis.

Out of the eight hundred questionnaires sent and five hundred and three valid questionnaires were returned from graduate and undergraduate students in eight private and public universities in Ghana. The return rate was 62.9%. Table 1 summarizes the characteristics of the respondents. The number of males (about 52%) and females (about 48%) provided almost a gender balance. The majority of the respondents were within the ages of 16 ad 25 years, accounting for 54.6%. The number of undergraduate respondents (about 70%) was over twice that of graduate (about 30%) respondents. Programs offered by the students cut across major disciplines in the university, with technology representing about 34%. Also, level 100 and 200 students form the highest number of participants, representing 47.7 percent.

RESULTS

Computer Ethics

The hypothesis 1 proposed that Consequence-based ethics (CBE), Duty-based ethics (DBE), and Character-based or Virtue ethics (VBE) will significantly explain and predict computer ethics. The hypothesis was tested using multiple regression analysis. In order to perform the test, multicollinearity and correlation were assessed. The variance inflation factor (VIF) was examined to determine

Table 1. Demographic characteristics of participants

Characteristics	Group	Frequency	Percentage
Gender	Male	263	52.3
	Female	240	47.7
Education	Undergraduate	351	69.8
	Graduate	152	30.2
Age	15 or less	7	1.4
	16-20	144	28.6
	21-25	131	26.0
	26-30	37	7.4
	31-40	87	17.3
	41-50	80	15.9
	Over 50	17	3.4
University	Private	200	39.8
	Public	303	60.2
National	International	41	8.2
	Local	462	91.8
Program	Technology	170	33.8
	Engineering	26	5.2
	Business Administration	111	22.1
	Theology	141	28.0
	Medical & Health Science	53	10.5
	Others	2	0.4
Level of Education	Level 100	101	20.1
	Level 200	139	27.6
	Level 300	61	12.1
	Level 400	95	18.9
	Level 500	7	1.4
	Level 600	82	16.3
	Level 700	10	2.0
	Level 800	2	0.4
	Others	6	1.2

n = 503

multicollinearity and Pearson correlation to assess the strength of the relationships among the variables. Variance inflation factor is an important measure that indicates multicollinearity. Multicollinearity occurs in regression analysis when there is a high correlation of at least one independent variable with a combination of other independent variables (Ringle et al., 2015). A VIF of 5 is considered the maximum level and 1 as the minimum (Ringle et al., 2015). The tests for multicollinearity in this study found low levels of multicollinearity (VIF = 1.74 for Consequence-based ethics, 1.93 for

Duty-based ethics, and 1.98 for Character-based ethics) (see Table 3). Accordingly, all the variables were within the acceptable level.

Following the acceptable level of VIF, each hypothesis was tested using Pearson Correlation and multiple regression analysis. Pearson's Correlation and multiple regression analyses were conducted to explain the significant effect of Consequence-based ethics, Duty-based ethics, and Character-based ethics on Computer Ethics. As can be observed from Table 3, each of the ethical theories was positively and significantly correlated with Computer Ethics. The multiple regression model with all the three predictors explained 29.78% of the variance and that the model was a significant predictor of Computer Ethics ($R^2 = .297$, $F_{(3, 499)} = 70.114$, $p < .001$). The final predictive model is shown below.

$$\text{Computer Ethics (CET)} = 1.297 + (.318 * \text{CBE}) + (.246 * \text{DBE}) + (.150 * \text{VBE}) + .219$$

Observably, the consequence-based and the duty-based ethics had the most significant ($p < .001$) positive regression weights of .318 and .246 respectively, indicating that higher scores on these scales would lead to a higher level of computer ethics, after controlling for the other variables in the model. Character-based ethics also had significant effect ($p < .01$) on computer ethics. Consequently, consequence-based ethics had the most significant effect on computer ethics (CET).

Cyber Privacy

A multiple regression was conducted to see whether Consequential ethics, Deontological ethics, and Virtue ethics would significantly explain Cyber Privacy (Hypothesis 2). Firstly, the assumptions for using multiple regression were tested. Correlation was conducted to examine the relationship between Cyber Privacy and the three predictors. Table 4 summarized the descriptive statistics (mean and standard), regression weights, correlation values, and the VIF. As can be seen, each of the predictors (Consequential Ethics, Deontological Ethics, and Virtue Ethics) positively and significantly correlated with Cyber Privacy. This indicates that the higher levels of predictors would result in a higher level of Cyber Privacy. A test to ascertain whether the data met the assumption of collinearity showed that multicollinearity was not a concern (Consequential Ethics, Tolerance = .575, VIF = 1.74; Deontological Ethics, Tolerance = .519, VIF = 1.93; Virtue Ethics, Tolerance = .505, VIF = 1.98). The data also met the assumption of independent errors (Durbin-Watson value = 1.738). An acceptable Durbin-Watson values can be anywhere between 0 and 4.

Secondly, the results from multiple regression analysis indicated that the model explained 24.5% of the variance and that the model was a significant predictor of Cyber Privacy, $F_{(3, 499)} =$

Table 2. Summary of statistics, correlation, and results from regression analysis

Variables	Mean	SD	Pearson's Correlation with CET	t	Sig.	Multiple Regression Weights			Collinearity Statistics	
						B	SE B	Beta β	Tolerance	VIF
Consequential Ethics (CBE)	4.40	.692	.488	5.727	.000	.318***	.056	.284	.575	1.74
Deontological Ethics (DBE)	4.46	.663	.464	4.037	.000	.246***	.061	.210	.519	1.93
Virtue Ethics (VBE)	4.19	.705	.443	2.579	.010	.150**	.058	.136	.505	1.98
Computer Ethics (CET)	4.42	.777								

N=503. Dependent Variable: CET; * $p < .05$ ** $p < .01$ *** $p < .001$; Consequential Ethics (CBE); Duty-Based Ethics (DBE); Virtue Ethics (VBE)

53.874, $p < .001$. The results also indicated that all the predictors were significant predictors of Cyber Privacy. Thus, Consequential Ethics (CBE) contributed significantly to the model ($B = .294$, $p < .001$), Deontological Ethics (DBE) ($B = .158$, $p < .01$), and Virtue Ethics (VBE) ($B = .171$, $p < .01$). The predictive model is:

$$\text{Cyber Privacy (PRI)} = 1.707 + (.294 * \text{CBE}) + (.158 * \text{DBE}) + (.171 * \text{VBE}) + .219$$

Noticeably, the Consequential Ethics was the largest significant predictor of the model. Controlling for the other predictors (Deontological Ethics and Virtue Ethics), as Consequential Ethics (CBE) increased Cyber Privacy increased most significantly.

Intellectual Property

Hypothesis 3 proposed that Consequential ethics, Deontological ethics, and Virtue ethics would significantly explain Intellectual Property rights. Table 5 summarized the descriptive statistics (mean and standard) and the correlation values. As shown in the table, each of the predictors positively and significantly correlated with Intellectual Property rights. This indicated that the higher scores on predictors would tend to have higher levels of Intellectual Property rights. The assumption of independent errors was acceptable (Durbin-Watson value = 1.773) and multicollinearity was not a concern (Consequential Ethics, Tolerance = .575, VIF = 1.74; Deontological Ethics, Tolerance = .519, VIF = 1.93; Virtue Ethics, Tolerance = .505, VIF = 1.98).

Multiple regression analysis was used to test whether Consequential ethics, Deontological ethics, and Virtue ethics would significantly explain Intellectual Property rights. The results of the test indicated that the three predictors (Consequential Ethics, Deontological Ethics, and Virtue Ethics) explained 28.2% of the variance ($R^2 = .282$, $F_{(3,499)} = 65.393$, $p < .001$). The test found that the Consequential Ethics significantly predicted Intellectual Property rights ($\beta = .245$, $p < .001$), as did Deontological Ethics ($\beta = .359$, $p < .001$), and Virtue Ethics ($\beta = .267$, $p < .001$). The final predictive model:

$$\text{Intellectual Property (IPR)} = .157 + (.245 * \text{CBE}) + (.359 * \text{DBE}) + (.267 * \text{VBE}) + .275$$

Table 3. Summary of statistics, correlation, and results from regression analysis

Variables	Mean	SD	Pearson's Correlation with PRI	t	Sig.	Multiple Regression Weights			Collinearity Statistics	
						B	SE B	Beta β	Tolerance	VIF
Consequential Ethics (CBE)	4.40	.692	.449	5.289	.000	.294***	.056	.271	.575	1.74
Deontological Ethics (DBE)	4.46	.663	.402	2.590	.010	.158**	.061	.140	.519	1.93
Virtue Ethics (VBE)	4.18	.705	.414	2.930	.004	.171**	.058	.160	.505	1.98
Cyber Privacy (PRI)	4.42	.750								

N=503. Dependent Variable: PRI * $p < .05$; ** $p < .01$; *** $p < .001$; Consequential Ethics (CBE); Deontological Ethics (DBE); Virtue Ethics (VBE).

Table 4. Summary of statistics, correlation, and results from regression analysis

Variables	Mean	SD	Pearson's Correlation with IPR	t	Sig.	Multiple Regression Weights			Collinearity Statistics	
						B	SE B	Beta β	Tolerance	VIF
Consequential Ethics (CBE)	4.40	.692	.435	3.507	.000	.245***	.070	.175	.575	1.74
Deontological Ethics (DBE)	4.48	.663	.474	4.673	.000	.359***	.077	.246	.519	1.93
Virtue Ethics (VBE)	4.18	.705	.459	3.637	.000	.267***	.073	.194	.505	1.98
Intellectual Property (IPR)	3.95	.968								

N=503. Dependent Variable: IPR; *p < .05; **p < .01; ***p < .001; Consequential Ethics (CBE); Deontological Ethics (DBE); Virtue Ethics (VBE).

In this model, the Deontological Ethics had the most significant positive effect, indicating that after accounting for Consequential Ethics and Virtue Ethics, participants with higher levels of Deontological Ethical perspective were expected to have a higher level of Intellectual Property right.

Academic Integrity

Finally, hypothesis 4 proposed that Consequential ethics, Deontological ethics, and Virtue ethics would significantly explain Academic Integrity. Correlation was first conducted to assess the relationship between Academic Integrity and the three predictors (Consequential Ethics, Deontological Ethics, and Virtue Ethics). Table 6 summarized the descriptive statistics (mean and standard), correlation values, regression weights, and the VIF. As can be observed from the table all the predictors positively and significantly correlated with Academic Integrity, indicating that the higher levels of scores on the predictors would tend to have a higher level of Academic Integrity. Tests of multicollinearity found that a low level of multicollinearity was present (VIF = 1.74 for Consequence-based ethics, 1.93 for Duty-based ethics, and 1.98 for Character-based ethics). The VIF of 5 is considered the maximum level and 1 as the minimum (Ringle et al., 2015). Accordingly, all the variables were within the acceptable level. When Academic Integrity was predicted, it was found that Consequential Ethics ($B = .141$, $p < .001$) and Virtue Ethics ($B = .125$, $p < .01$) were the significant predictors. However, Deontological Ethics was not a significant predictor of Academic Integrity ($B = .031$, ns).

The multiple regression model with all the three predictors explained 16.5% of the variance and that the model was a significant predictor of Academic Integrity ($R^2 = .165$, $F(3, 499) = 32.751$, $p < .001$). The final predictive model is as below.

$$\text{Academic Integrity (AIT)} = 2.504 + (.141 * \text{CBE}) + (.031 * \text{DBE}) + (.125 * \text{VBE}) + .137$$

The Consequential Ethics had the most significant positive effect on Academic Integrity, indicating that after accounting for Deontological Ethics and Virtue Ethics, participants with higher levels of Consequential Ethical perspective were expected to have a higher level of Academic Integrity.

DISCUSSION

Results from the study reveal that all the four regression models are statistically significant. Particularly, consequential ethics, deontological ethics, and virtue ethics significantly predict and explain computer

Table 5. Summary of statistics, correlation, and results from regression analysis

Variables	Mean	SD	Pearson's Correlation with AIT	t	Sig.	Multiple Regression Weights			Collinearity Statistics	
						B	SE B	β	Tolerance	VIF
Consequential Ethics (CBE)	4.40	.692	.364	4.053	.000	.141***	.035	.219	.575	1.740
Deontological Ethics (DBE)	4.48	.663	.302	.806	.421	.031	.038	.046	.519	1.925
Virtue Ethics (VBE)	4.18	.705	.359	3.436	.001	.125**	.036	.198	.505	1.982
Academic Integrity (AIT)	3.79	.447								

N=503. Dependent Variable: AIT; *p < .05 **p < .01 ***p<.001; Consequential Ethics (CBE); Deontological Ethics (DBE); Virtue Ethics (VBE).

ethics, cyber privacy, intellectual property rights, and academic integrity. This suggests that all the ethical theories in the models could be used to predict cyber ethics. Thus, when people are faced with ethical dilemma, they tend to apply these theories in their judgement. According to Curzer et al. (2014), people regularly use various moral and ethical theories at different times for decision-making.

In particular, the three ethical theories explain (as represented by the R-Squared) and predict cyber ethics (computer ethics, cyber privacy, intellectual property, and academic integrity) at various degrees. Overall, consequential ethics, deontological ethics, and virtue ethics explain about 30, 25, 28, and 17 percent of computer ethics, cyber privacy, intellectual property, and academic integrity respectively (see Table 7). The R-squared values are generally low for all the four models. However, in the studies that predict human behaviour, it is entirely expected that R-squared values will be low (Onditi, 2013). This is because humans are simply harder to predict as compared with physical processes (Onditi, 2013). Though the R-squared values are low, the models have statistically significant predictors. Therefore, important conclusions can be made as to how changes in the predictors are associated with changes in the outcome variable.

Observably, consequential ethics is the most significant predictor of computer ethics, cyber privacy, and academic integrity. That is, apart from Model 3 (ethical theories on intellectual property), consequential ethics was found to be the most statistically significant predictor of Model 1 (ethical theories on computer ethics), Model 2 (ethical theories on cyber privacy), and Model 4 (ethical theories on academic integrity). This suggests that consequential ethics play a major role in cyber ethics. Consequences attached to intellectual property rights laws, cyber privacy laws, cybercrime laws, and repercussions of academic dishonesty might explain the contribution of consequential ethics to the models.

The utilitarianism view of consequential ethics suggest that an act is morally permissible if the consequences resulting out of it produces greatest amount of good for the greatest number of persons affected (Heller, 2012). Apparently, this view could contribute to cyber ethics behaviour of users in the cyberspace. Group consequentialism is another view of consequential ethics. It considers consequences of an act on smaller groups such as a nation (Hinmann, 2016). This means that people's ethical choices in the cyberspace depends on the consequences the actions would have on the small groups. In this case, people might choose ethically to protect their groups. The third aspect of consequentialism is ethical egoism, which focuses on the consequences of an action on oneself (Hinmann, 2016). Thus, when people consider the consequences of the actions in the cyberspace on themselves, they may choose to act ethically

Table 6. Explanation and prediction power of the models

Model	Criterion	Predictors	B	R ²
1	Computer Ethics	Consequential Ethics	.318***	29.7%
		Deontological Ethics	.246***	
		Virtue Ethics	.150**	
2	Cyber Privacy	Consequential Ethics	.294***	24.5%
		Deontological Ethics	.158**	
		Virtue Ethics	.171**	
3	Intellectual Property	Consequential Ethics	.245***	28.2%
		Deontological Ethics	.359***	
		Virtue Ethics	.267***	
4	Academic Integrity	Consequential Ethics	.141***	16.5%
		Deontological Ethics	.031	
		Virtue Ethics	.125**	

*p < .05; **p < .01; ***p < .001

Also, deontological ethics is the most significant predictor of intellectual property rights preservation. Deontological ethics propose that to act ethically, one ought to follow the appropriate rules, which is the right course of action for the performance of one's duty (Alexander & Moore, 2015). Perhaps, the codes of ethics and laws that protect intellectual property rights account for people's moral judgment in the cyberspace.

CONCLUSION

The current study focussed on three ethical theories and four cyber ethics. Consequential ethics was the most significant predictor of computer ethics, cyber privacy, academic integrity, and the deontological ethics was the most significant predictor of intellectual property right. The largest observed measure of the extent to which the theories explain cyber ethics was 30 percent. This suggested that there were other theories that might contribute significantly to cyber ethics but were not included in the models. Also, some cyber ethics constructs were not included in the current study, such as cyber harassment, cyberbullying, hate speech, and predatory. These would be examined in future work. Moreover, longitudinal study is required as people do not use one theory all the time, but rather discards a particular theory in favour of another at different times. This study has implication for theory and practice. Theoretically, the study applied ethical theories to predict and explain cyber ethics. Researchers could explore further by including other theories and in different settings to confirm or extend the current findings. Practically, cyber ethics educators could integrate ethical theories into cyber ethics education to guide people who use the cyberspace to do so in ethical manner.

REFERENCES

- Abu-Shaqra, B., & Luppiciini, R. (2016). Technoethical Inquiry into Ethical Hacking at a Canadian University. *International Journal of Technoethics*, 7(1), 62–76. doi:10.4018/IJT.2016010105
- Alexander, L., & Moore, M. (2015). Deontological ethics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Spring 2015 ed.). Stanford University Press. Retrieved from <http://plato.stanford.edu/archives/spr2015/entries/ethics-deontological/>
- Amin, Z. (2019). A practical road map for assessing cyber risk. *Journal of Risk Research*, 22(1), 32–43. doi:10.1080/13669877.2017.1351467
- Association for Computing Machinery. (2018). *ACM code of ethics and professional conduct*. Retrieved from <https://www.acm.org/code-of-ethics>
- Audi, R. (2015). Virtue ethics in theory and practice. In *Reasons, Rights, and Values* (pp. 203–226). Cambridge: Cambridge University Press. doi:10.1017/CBO9781316156766.010
- Barger, R. (2008). Privacy Concerns. In *Computer Ethics: A Case-based Approach* (pp. 177–185). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511804151.015
- Bentham, J. (1970). *An introduction of the principles of morals and legislation*. Oxford, UK: The Athlone Press.
- Burmeister, O. K. (2013). Achieving the goal of a global computing code of ethics through an international-localisation hybrid, Ethical Space. *The International Journal of Communication Ethics*, 10, 25–32.
- Buttyán, L., & Hubaux, J. (2007). Privacy protection. In *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing* (pp. 237–272). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511815102.010
- Charoensukmongkol, P., Daniel, J. L., Sexton, S., & Kock, N. (2012). Analyzing Software Piracy from Supply and Demand Factors The Competing Roles of Corruption and Economic Wealth. *International Journal of Technoethics*, 3(1), 28–42. doi:10.4018/jte.2012010103
- Christakis, E., & Christakis, N. A. (2012). *Harvard Cheating Scandal: Is Academic Dishonesty on the Rise?* Retrieved from <http://ideas.time.com/2012/09/04/harvard-cheating-scandal>
- Churchill, R. P. (2019). Ghosts in the Machine?: On the Limits of Narrative Identity in Cyberspace. *International Journal of Technoethics*, 10(1), 10–23. doi:10.4018/IJT.2019010102
- Computer Ethics Institute. (1992). *Ten commandments of computer ethics*. Retrieved from <http://computerethicsinstitute.org/publications/tencommandments.html>
- Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: A risk-based systems approach to cyber decisions. *Environment Systems & Decisions*, 33(4), 469–470. doi:10.1007/s10669-013-9484-z
- Copyright Act. (2005). *Copyright Act 2005*. Retrieved from <https://www.aripo.org/wp-content/uploads/2018/12/Ghana-Copyright-Act.pdf>
- Curzer, H. J., Sattler, S., DuPree, D. G., & Rachelle Smith-Genthôs, K. (2014). Do ethics classes teach ethics? *School Field*, 12(3), 366–382.
- Cybersecurity Ventures (2019). *Cybercrime Damages \$6 Trillion By 2021*. Retrieved from <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- Data Protection Commission. (2012). The Data Protection Act, 2012 (Act 843). Retrieved from <https://www.dataprotection.org.gh/index.php/data-protection/data-protection-acts-2012>
- Dhusia, D. K. (2017). Strategies for preventing plagiarism - A case study of top Indian universities. *Global Journal of Enterprise Information System*, 9(2), 84–87. doi:10.18311/gjeis/2017/16191
- Dipert, R. R. (2016). Distinctive Ethical Issues of Cyberwarfare. In F. Allhof, A. Henschke, & B. J. Strawser (Eds.), *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780190221072.003.0004

Driver, J. (2014). The history of utilitarianism. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Winter 2014 ed.). Stanford University Press. Retrieved from <http://plato.stanford.edu/archives/win2014/entries/utilitarianism-history/>

Dunne, R. (2009). The Right of Privacy. In *Computers and the Law: An Introduction to Basic Legal Principles and Their Application in Cyberspace* (pp. 194–237). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511804168.010

Engelbreton, P. (2011). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy* (1st ed.). Syngress.

Ethics guide. Introduction to ethics. (2014). BBC. Retrieved from <http://www.bbc.co.uk/ethics/introduction/>

Pruitt-Mentle, D. (2008). *National Cyberethics, Cybersafety, Cybersecurity Baseline Study. Educational Technology Policy Research and Outreach (ETPRO), National Cyber Security Alliance*. NCSA.

García-Matos, M., & Torner, L. (2015). Privacy. In *The Wonders of Light* (pp. 81–88). Cambridge: Cambridge University Press. doi:10.1017/CBO9781316151075.013

Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics*, 3(1), 14–27. doi:10.4018/jte.2012010102

Hennig, N. (2018). Privacy and security online: Best practices for cybersecurity. *Library Technology Reports*, 54(3), 1–37.

Henseler, J., & Sarstedt, M. (2012). Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics*, 28(2), 565–580. doi:10.1007/s00180-012-0317-1

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. doi:10.1007/s11747-014-0403-8

Hinman, L. M. (2016). *Contemporary Moral Issues: Diversity and Consensus*. Boston: Taylor and Francis. doi:10.4324/9781315509938

Indvik, L. (2013). 92% of e-book downloads in Russia are pirated. Mashable. Retrieved from <https://mashable.com/2013/07/09/russia-ebook-piracy/>

Jamal, A., Ferdoos, A., Zaman, M., & Hussain, M. (2015). Cyber-ethics and the perceptions of Internet users: A case study of university students of Islamabad. *Pakistan Journal of Information Management & Libraries*, 16, 8–20.

Kant, I. (1993). *Grounding for the metaphysics of morals* (3rd ed., J.W. Ellington, trans.). Indianapolis, IN: Hackett.

Kant, I. (1998). *Critique of Pure Reason*. Cambridge: Cambridge UP. doi:10.1017/CBO9780511804649

Lonsdale, D. J. (2016). Britain's Emerging Cyber-Strategy. *The RUSI Journal*, 161(4), 52–62. doi:10.1080/03071847.2016.1232880

Luppici, R. (2009). The Emerging Field of Technoethics. In *Handbook of Research on Technoethics*. Hershey, PA: IGI Global. doi:10.4018/978-1-60566-022-6.ch001

McDonald, G. (2014). Ethical theory. In *Business Ethics: A Contemporary Approach* (pp. 307–340). Cambridge: Cambridge University Press. doi:10.1017/CBO9781107445666.015

Mill, J. S. (1998). *Utilitarianism, edited with an introduction by Roger Crisp*. New York, NY: Oxford University Press.

Mill, S. J. (1961). *Utilitarianism*. Doubleday.

Monteverde, S. (2014). Undergraduate healthcare ethics education, moral resilience, and the role of ethical theories. *Nursing Ethics*, 21(4), 385–401. doi:10.1177/0969733013505308 PMID:24311237

Moore, R., & McMullan, E. C. (2009). Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students. *International Journal of Cyber Criminology*, 3(1), 441–451.

- Nasuti, H. P. (2018). Called into Character: Aesthetic and Ascetic Aspects of Biblical Ethics. *Catholic Biblical Quarterly*, 80(1), 1–24. doi:10.1353/cbq.2018.0000
- Novotney, A. (2011). Beat the cheat: Psychologists are providing insight into why students cheat and what faculty, schools and even students can do about it. *American Psychological Association*, 42(6), 54.
- Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York, NY: McGraw-Hill.
- Omosalewa, A., Aasheim, C. L., & Rutner, P. (2013). Development and Testing of a Survey Instrument to Assess Ethical Perceptions of IT and IS Students. *Information Technology Faculty Publications*, 9. Retrieved from <https://digitalcommons.georgiasouthern.edu/information-tech-facpubs/9>
- Onditi, A. A. (2013). Relationship between customer personality, service features and customer loyalty in the banking sector: A survey of banks in Homabay County, Kenya. *International Journal of Business and Social Science*, 4(15), 132–150.
- Onyancha, O. B. (2015). An informetrics view of the relationship between internet ethics, computer ethics and cyberethics. *Library Hi Tech*, 33(3), 387–408. doi:10.1108/LHT-04-2015-0033
- Ozolinš, J. (2015). Ethical theories. In J. Ozolinš & J. Grainger (Eds.), *Foundations of Healthcare Ethics: Theory to Practice* (pp. 14–32). Cambridge: Cambridge University Press. doi:10.1017/CBO9781107589834.002
- Perez-Pena, R. (2012, August 31). Harvard Students in Cheating Scandal Say Collaboration Was Accepted. *The New York Times*.
- Reeves, G. (2010). *Off-duty discussion groups can be off-limits to employers*. 4Hoteliers. Retrieved from http://www.4hoteliers.com/4hots_fshw.php?mwi=4880
- Schultz, R. A. (2010). IT-Enabled Global Ethical Problems. In R. Schultz (Ed.), *Information Technology and the Ethics of Globalization: Transnational Issues and Implications*. Hershey, PA: IGI Global.
- Shiffrin, S. (2016). Privacy. In *What's Wrong with the First Amendment* (pp. 13–24). Cambridge: Cambridge University Press. doi:10.1017/CBO9781316676042.002
- Sinnott-Armstrong, W. (2014). Consequentialism. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Spring 2014 ed.). Stanford University Press. Retrieved from <http://plato.stanford.edu/archives/spr2014/entries/consequentialism/>
- Spinello, R. A., & Tavani, H. (Eds.). (2004). *Readings in Cyberethics*. Sudbury, MA: Jones and Bartlett Publishers.
- Stamatellos, G. (2011). Computer ethics and neoplatonic virtue: A reconsideration of cyberethics in the light of Plotinus' ethical theory. *International Journal of Cyber Ethics in Education*, 1(1), 1–11. doi:10.4018/ijcee.2011010101
- Sulphey, M. M., & Jnaneswar, K. (2013). A study on the academic dishonesty, anomia and unethical behaviour among business graduates. *Journal of Contemporary Management Research*, 8(2), 57–72.
- Swartz, L. B., & Cole, M. T. (2013). Students' perception of academic integrity in online business education courses. *Journal of Business and Educational Leadership*, 4(1), 102–112.
- Talbot, M. (2012). Ethical theories: Virtue, duty and happiness. In *Bioethics: An Introduction* (pp. 32–49). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139047234.008
- Taylor, S. A. (2012). Evaluating digital piracy intentions on behaviours. *Journal of Services Marketing*, 26(7), 472–483. doi:10.1108/08876041211266404
- Tiirmaa-Klaar, H. (2016). Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*, 1(1), 94–106. doi:10.1080/23738871.2016.1165716
- Tomczyk, L. (2019). The Practice of Downloading copyrighted files among adolescents in Poland: Correlations between piracy and other risky and protective behaviours online and offline. *Technology in Society*, 58.
- Verrier, R. (2013). Online piracy of entertainment content keeps soaring. *LA Times*. Retrieved from <https://www.latimes.com/entertainment/envelope/cotown/la-fi-ct-piracy-bandwidth-20130917-story.html>

APPENDIX A. TABLE 2

Table 7. Cyber Ethics Questionnaire

	Consequence-Based Ethics <i>I consider the CONSEQUENCES (RESULTS) OF MY ACTIONS on myself and/or on others and as such:</i>	Factor Loading	Cronbach's Alpha
1	I shall not use a computer to harm other people.	.724	.88
2	I shall not interfere with other people's computer work.	.779	
3	I shall not snoop around in other people's computer files.	.751	
4	I shall not use a computer to steal.	.744	
5	I shall not use a computer to bear false witness.	.789	
6	I shall not copy or use proprietary software for which I have not paid for.	.776	
7	I shall not use other people's computer resources without authorization or proper compensation.	.720	
8	I shall not appropriate other people's intellectual output.	.709	
9	I shall think about the social consequences of the program I am writing, the system I am designing, or the systems I am using.	.703	
10	I shall always use a computer in ways that ensure consideration and respect for my fellow human beings.	.737	
	Duty-Based Ethics <i>I feel it is the RIGHT THING TO DO and as such:</i>		.90
1	I shall not use a computer to harm other people.	.747	
2	I shall not interfere with other people's computer work.	.796	
3	I shall not snoop around in other people's computer files.	.758	
4	I shall not use a computer to steal.	.743	
5	I shall not use a computer to bear false witness.	.724	
6	I shall not copy or use proprietary software for which I have not paid for.	.736	
7	I shall not use other people's computer resources without authorization or proper compensation.	.704	
8	I shall not appropriate other people's intellectual output.	.794	
9	I shall think about the social consequences of the program I am writing, the system I am designing, or the systems I am using.	.785	
10	I shall always use a computer in ways that ensure consideration and respect for my fellow human beings.	.749	
	Character-Based Ethics <i>It is my MORAL CHARACTER and as such:</i>		.92
1	I shall not use a computer to harm other people.	.784	
2	I shall not interfere with other people's computer work.	.831	
3	I shall not snoop around in other people's computer files.	.826	
4	I shall not use a computer to steal.	.784	
5	I shall not use a computer to bear false witness.	.772	
6	I shall not copy or use proprietary software for which I have not paid for.	.760	
7	I shall not use other people's computer resources without authorization or proper compensation.	.736	
8	I shall not appropriate other people's intellectual output.	.714	
9	I shall think about the social consequences of the program I am writing, the system I am designing, or the systems I am using.	.729	
10	I shall always use a computer in ways that ensure consideration and respect for my fellow human beings.	.756	
	Academic Integrity <i>I believe it is UNETHICAL to:</i>	Factor Loading	.88
1	Take credit for someone else's work.	.757	
2	Hire someone over the Internet to write a term paper, project, or an essay for me.	.796	
3	Purchase or submit a research or term paper from the Internet to a class as one's own work.	.764	
4	Use the Internet to cheat on a graded assignment or examination.	.769	
5	Plagiarize other people's work without citing or referencing the work.	.704	
6	Add the name of a non-contributing person as an author in a project or research study.	.783	
7	Copy and paste material found on the Internet for an assignment without acknowledging the authors of the material.	.713	
8	Deliberately provide inaccurate references for a project or research study.	.779	
9	Submit work done by another student as one's own.	.722	
	Computer Ethics <i>I shall NOT:</i>		

continued on following page

Table 7. Continued

	Consequence-Based Ethics <i>I consider the CONSEQUENCES (RESULTS) OF MY ACTIONS on myself and/or on others and as such:</i>	Factor Loading	Cronbach's Alpha
1	Hack into a computer system to obtain passwords, corrupt files, download programs, etc.	.824	.88
2	Take on different identity on the Internet for fun or profit (e.g., to perform credit card fraud).	.873	
3	Using social media networking as a tool for cyber bullying is unethical.	.780	
4	Send files infected with viruses over the Internet.	.790	
5	Steal funds electronically or by the use of the Internet.	.814	
	Cyber Privacy <i>I shall NOT:</i>		
1	Disclose confidential institutional information to others without authorization.	.772	.85
2	Spread the wrong information about other people by means of the Internet.	.734	
3	Violate the privacy and confidentiality of information (e.g. trade secret, password) entrusted to me to further personal interest.	.794	
4	Obtain another person's private files by means of the Internet.	.811	
5	Read someone else's email or WhatsApp message without their permission	.710	
6	Use technology to infringe on other people privacy rights.	.786	
7	Collect and share information about other people over the Internet without their prior consent.	.735	
	Intellectual Property Rights <i>I believe it is UNETHICAL to</i>		
1	Download and/or distribute copyrighted materials (e.g. software, e-books, video, and audio) to other people over the Internet.	.863	.78
2	Copy an entire article from the Internet and turning it in as one's own assignment.	.796	
3	Buy software with a single user license and then install it on multiple computers.	.837	

Winfred Yaokumah is a researcher and senior faculty at the Department of Computer Science of the University of Ghana. He has published books, book chapters, 4 conference papers, and several articles in highly rated journals including "Information and Computer Security," "Information Resources Management Journal," IEEE Xplore, "International Journal of Human Capital and Information Technology," "International Journal of Human Capital and Information Technology Professionals," "International Journal of Technology and Human Interaction," "International Journal of e-Business Research," "International Journal of Enterprise Information Systems," "Journal of Information Technology Research," "International Journal of Information Systems in the Service Sector," and "Education and Information Technologies." His research interest includes cyber security, cyber ethics, network security, and information systems security and governance. He serves as a member of the International Review Board for the "International Journal of Technology Diffusion."